ABSTRACT

A method of cyphering and/or decyphering, by an integrated circuit, of a digital input code by means of several keys, consisting of: dividing said code into several data blocks of same dimensions; and applying to said blocks several turns of a cyphering or decyphering consisting of submitting each block to at least one same non-linear transformation and of subsequently combining each block with a different key at each turn, the operands being masked, upon execution of the method, by means of at least one first random number having the size of said code and all the blocks of which have the same value by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said random number.